Amendments to the Drawings:

Please add the attached new sheet of drawing for Figure 1. No new matter has been added. The specification text as amended now refers on page 7 to the new figure.

REMARKS

Claims 1, 13-15, and 17-21 are pending in the present application. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

The Office Action required that Applicant add a drawing to facilitate understanding of the invention. A new sheet of drawing has been added according to the Examiner's requirements. Additionally, the specification text has been amended so as to refer to this new figure. No new matter has been added.

Claim 17 was objected to because claim 17 allegedly disclosed the method claim 14 yet the limitations disclosed in claim 17 seem to depend on the limitations of claim 15. Claim 17 has been amended to depend from claim 15. Withdrawal of the objection is respectfully requested.

Claims 1, 13-15 and 17-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Griffin et al. (U.S. Patent No. 5,249,294) in view of Kocher et al. (U.S. Patent Publication No. 2002/0124178 herein after Kocher. These rejections are respectfully traversed for the following reasons.

Claim 1 recites method for securing a computer system which comprises at least a code interpretation module and memory capacities for storing an interpreted code having measurable physical imprints, wherein in order to make more difficult attacks based on physical measurements or requiring synchronization with the interpreted code, the method comprises the steps of providing at least two different implementations for at

least one instruction of the interpreted code, the different implementations each requiring a different execution time and/or having a different physical imprint while providing an identical result, selecting one of the different implementations to be executed before each execution of the instruction, and executing the determined different implementation. This is not taught, disclosed or made obvious by the prior art of record.

In the Office Action, claim 1 was rejected on the alleged ground that it would have been obvious to one having ordinary skill on the art at the time of the applicant's invention to combine the teaching of Kocher within the system of Griffin because "code interpretation module allows different high level language programs to be executed in a single platform". Applicant respectfully disagrees.

The objective of the method disclosed in Griffin is to inhibit synchronization of a "predetermined secure data processing routine" (routine to be protected) with an external event by preventing the determination of the time when this routine will be executed. To achieve this goal, Griffin proposes to execute one or more interim routines between the occurrence of the event and the routine to be protected [Figure 1 and Column 2 lines 55-58]. As described in Griffin [Figure 2 and Column 3, lines 64-68], the purpose of these interim routines is only to provide a delay: as a result, they typically do not do any computation except for decrementing a counter.

In contrast with Griffin, the method according to Applicant's invention does not suggest the introduction of interim routines. Instead, the method relies on the existence of an interpretation code module for the interpretation of instructions and includes of proposing a plurality of implementations of certain instructions each requiring

a different execution time and/or having a different physical imprint and providing an identical result. As a consequence, Griffin does not disclose and cannot suggest the essential features of the method recited in Claim 1 of Applicant's invention.

The method recited in Claim 1 essentially relies on the plurality of implementations of instructions (the instructions used in the code of the "predetermined secure data processing routine" in Griffin's terms). In contrast, Griffin does not disclose such multiplicity of implementations of instructions but proposes instead the introduction of interim "void" routines to be executed before the "predetermined secure data processing routine". This explains why the method according to Applicant's invention relies in an essential way on the existence of an interpretation code module whereas Griffin does not rely on such an assumption.

The method proposed in Claim 1 leaves the code to the software (the code including the "predetermined secure data processing routine") unchanged, whereas the introduction of branches to interim routines proposed in Griffin implies that the code of the software has to be modified.

The method claimed in Applicant's Claim 1 modifies the physical imprint or execution time of the "predetermined secure data processing routine" (because of the variations in the physical imprints of the instructions used to implement it), whereas Griffin delays the execution of this "predetermined secure data processing routine" but does not modify its own physical imprint or execution time.

Kocher discloses a system for evaluating the security of a cryptographic device to recover useful information about a key as well as a method for analyzing

externally measurable characteristics of a cryptographic device containing a secret key to recover information about that key. In this respect, Kocher proposes to connect the cryptographic device to an analog to digital converter configured to measure the externally measurable characteristics of the cryptographic device. This system is adapted to send command sequences to the cryptographic device to determine whether information about a key contained in this device is leaked.

However, it could be also used by intruders to attack computer systems on the basis of a physical measurement as stated in Applicant's specification (see the background section). Applicant's claimed invention is intended to render such attacks more difficult or even impossible.

In the cited document, Kocher discloses several known techniques used for protecting cryptosystems (i.e., countermeasures) such as: reduction of signal to noise ratio; Random Noise Generation Clock Skipping, Execution Path and Operation Order Entropy (Input Order Permutation – Blinded High Entropy Permutation). However, none of these techniques corresponds to the method as claimed in Applicant's claim 1. In fact, Applicant respectfully submits that the system disclosed by Kocher is related to Applicant's method only to the extent it refers to Java Interpreted code.

For these reason the combination of teaching from Griffin et al and from Kocher et al cannot conduce to Applicant's claimed solution, but to a solution for preventing the time of execution of a predetermined routine included in an overall larger data processing routine from being determined, such a solution using a Java interpreted code and comprising:

a) providing a random-content signal during each overall larger data processing routine; and

b) varying the duration between an occurrence of the externally observable event and the execution of the predetermined routine during each overall larger data processing routine in response to said random-content signal.

As previously explained such a solution does not correspond to Applicant's claimed solution, which uses a code interpretation module and which provides several implementations for at least one instruction of the interpreted code.

For at least this reason, the proposed combination of Griffin and Kocher would not have rendered claim 1 obvious, as well as claims 13-15 and 17-21, which depend from claim 1. For at least these reasons, Applicant respectfully submits that claims 1, 13-15 and 17-21 are patentable over the prior art of record whether taken alone or in combination as proposed in the Office Action.

In view of the above amendment and remarks, Applicant respectfully requests reconsideration withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to the effect is most earnestly solicited.

If the Examiner has any questions, he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:srd
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\M\Mout\HAMEAU2\pto\2008-06-06Amendment.doc